International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

A study on role of Cryptography in Blockchain System

N.Vijay kumar
Assistant Professor, Dept. of CSE,
SR Engineeing College, Warangal
P.Kumaraswamy
Assistant Professor, Dept. of CSE,
SR Engineeing College, Warangal
palleboina.kumar@gmail.com
S.Vahini
Assistant Professor, Dept. of CSE,
S R Engineeing College, Warangal

***Abstract*— most cryptocurrencies serve completely different purposes than sending secret messages, but cryptography still plays a key role. Hashing is a cryptographic method for transforming large amounts of data into short numbers that are difficult to imitate. It is a key component of blockchain technology and is mainly concerned with the protection and integrity of the data flowing through the blockchain.**

Keywords- cryptograhy; hashing; blockchain; security;

I. INTRODUCTION

Asymmetric cryptography or public cryptography is an essential component of cryptocurrencies like Bitcoin and Ethereum [3].These advanced cryptographic techniques ensure that the source of transactions is legitimate and that hackers cannot steal user's funds. Here's an in-depth look at how blockchains accomplish this with public key cryptography**:**. Public Key Cryptography is a cryptographic system that relies on a pair of keys, a private key which is kept secret and a public key which is broadcasted out to the network. This system helps ensure the authenticity and integrity of a message by relying on advanced cryptographic techniques.

Public Key Cryptography is an essential part of Bitcoin's protocol and is used in several places to ensure the integrity of messages created in the protocol. Wallet creation and signing of transactions, which are the core components of any currency rely heavily on public key cryptography. Bitcoin's protocol uses what's called the Elliptic Curve Digital Signature Algorithm (ECDSA) to create a new set of private key and corresponding public key. The public key is then used with a hash function to create the public address that Bitcoin users use to send and receive funds. The private key is kept secret and is used to sign a digital transaction to make sure the origin of the transaction is legitimate

Digital signatures are quite similar to actual signatures on a document. They help ensure that the author of a transaction is, in fact, the individual who holds the private key. Digital signatures are the backbone of Bitcoin and every transaction has a different digital signature that depends on the private key of the user. Also, given the message, the public key of the user and the signature, it is non-trivial to check if the signature is authentic. More formally, digital signatures depend on two functions:

Sign (Message, Private Key) -> Signature

Given the message we want to sign and a private key, this function produces a unique digital signature for the message.

Verify (Message, Public Key, Signature) -> True/False

Given the message we want to verify, the signature and the public key, this function gives a binary output depending on whether the signature is authentic

Once the transaction is signed by the owner, the transaction is sent to the memory pool where it sits to be processed by miners. The miners use the sender's public key to ensure that the digital signature is authentic so that a hacker cannot spend a user's funds without their consent. If the ownership and digital signature check out, they include the transaction in the next block, and the money is sent from one wallet to another.

The other major use of cryptography in the Bitcoin protocol is in computing the proof of work

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

function. Miners rely on computing the "SHA256 Hash Function" for a lot of inputs until they find the nonce for a given block before adding it to the blockchain. The difficulty of the mining process is changed by how many zeroes the hash must begin with to be added to the blockchain. This is a unique system as it adjusts higher or lower depending on how many people are mining at any given time. It also makes it computationally infeasible for an attack vendor to go and edit transactions that are already recorded on the blockchain.

Crypto currencies use a peer-to-peer decentralized system to conduct transactions. Since the entire process is online, there are fears that the transactions maybe volatile and hackable. What we are going to see in this paper is how cryptocurrency uses cryptography to make their transactions extremely secure [2].

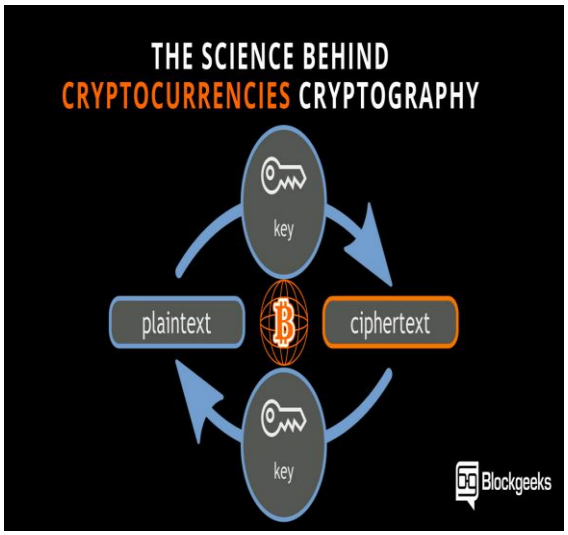

Figure1: Relation between cryptography and cryptocurrencies

Cryptography is a method of using advanced mathematical principles in storing and transmitting data in a particular form so that only those, for whom it is intended for, can read and process it. Cryptography has been used for thousands and thousands of years by people to relay messages without detection. In fact, the earliest use of cryptography was seen in the tomb taken from Old Kingdom in Egypt circa 1900 BCE. Cryptography has existed in the modern society through one way or another.

Encryption is one of the most critical tools used in cryptography. It is a means by which a message can be made unreadable for an unintended reader and can be read only by the sender and the recipient. In modern technology, there are three forms of encryption that are widely used, symmetric cryptography, asymmetric cryptography, and hashing.

II. SYMMETRIC CRYPTOGRAPHY AND ASYMMETRIC CRYPTOGRAPHY

There are two types of commonly used cryptosystems in cryptography [1]: Symmetric key and public key cryptosystems. Symmetric cryptography is the earliest known cryptographic method known to man. The concept is very simple and if we were to break it down to steps, this is what it will look like:

- You have a message M that you want to send over to your friend.
- You encrypt the message with a Key and get a cipher text C.
- Your friend gets your cipher text C.
- She then decrypts the cipher text using the same Key to retrieve message M.

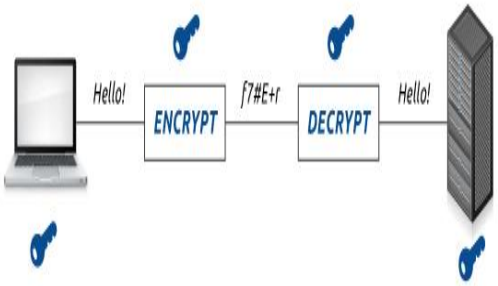

Figure2: Symmetric key cryptosystem

Even though symmetric cryptography has some major problems (which we will discuss in a bit) the biggest advantage of symmetric cryptography is that it requires very little overhead. You just need to share one single key with your recipient to go forward with this method.

Even now, a lot of software use this method in conjunction with asymmetric cryptography to provide fast and efficient encryption/decryption services.

Even though the overhead is significantly lesser, there are a lot of problems with symmetric cryptography.

Problem 1: The shared key

The fact that the encryption and decryption is done with one single key is a huge problem. First and foremost, the sharing of the key needs to be done in a much secured manner, if anyone gets hold the of key then all your data will be compromised.

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

Problem 2: It is not scalable

Another huge problem with symmetric cryptography is that it is not scalable at all. Suppose Alice runs an information center and sends data via symmetric key cryptography. It's ok if she is only dealing with 3-4 clients. But the most clients she gets, the more unique public keys she will have to handle and take care of. Eventually, it will become too much to handle. Because of these vulnerabilities of symmetric key cryptography, a solution was needed, and in the 1970's it finally came in the form of Public key cryptography (Asymmetric key cryptography).

Public-key encryption is a cryptographic system that uses two keys -- a *public key* known to everyone and a *private* or *secret key* known only to the recipient of the message.

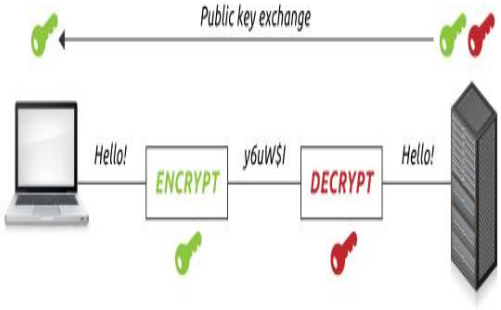

Figure3: Asymmetric key cryptosystem

An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

III. HASHING AND DIGITAL SIGNATURE

Hashing is a cryptographic method for transforming large amounts of data into short numbers that are difficult to imitate [5]. It is a key component of **blockchain technology** and is mainly concerned with the protection and integrity of the data flowing through the blockchain.
This method is mainly used for four processes:

- to verify and validate the account balances of wallets
- to encode wallet addresses
- to encode transactions between wallets
- to make the mining of blocks possible (for mineable cryptocurrencies) by creating the mathematical puzzles that need to be solved to solve a block

A digital signature, similar to your own signature, is used to verify that you are who you say you are. When it comes to cryptocurrencies, digital signatures are mathematical functions that are matched to a specific wallet.
Thus, they function as proof that a specific wallet is actually the wallet it claims to be – essentially, it's a digital identification of a wallet. By attaching a digital signature to a transaction, no one can dispute that that transaction came from the wallet it purports to have come from, and that wallet can't be impersonated by another wallet.

Digital signatures use cryptography for wallet identification and secretly match the public and private key of a wallet. Your public key is basically your bank account number, while your private key is the pincode. It doesn't matter if people know your bank account, because the only thing they can do with it is deposit money to your account. However, if they know your pincode too, you can have a real problem.

In blockchain, the private key is used for the encryption of transactions, while the public key is used for the decryption. This is possible because the sending party is the one responsible for a transaction. The sending party encrypts the transaction with their private key, but this can be decrypted with the recipient's public key because they only need to verify that it was indeed you who sent the message. If the sending party's public key doesn't work to decrypt the transaction, then the transaction isn't from that wallet [4].

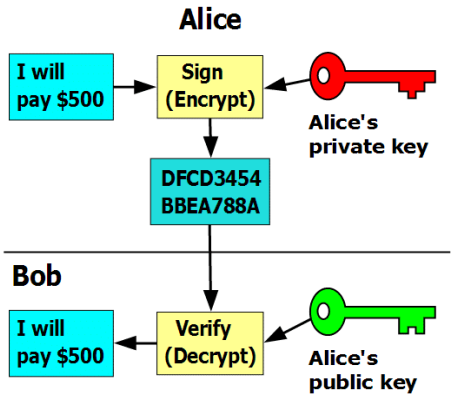

Figure 4: Digital signature

In this system, the public key is distributed freely and is paired secretly to a private key. It is not a

International Journal of Research
Available at https://pen2print.org/index.php/ijr/
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

problem if a public key is known, but the private key must always be kept a secret. Even though the two are paired, calculating someone's private key based on their public key is computationally so challenging that it's financially and technically infeasible.

Protecting the key is a main disadvantage of this method. If others learn your private key, they can access your wallet and make transactions with it, which actually happened in the **Bloomberg blunder** when a reported accidentally showed his private key on TV.

IV. FUNCTIONING OF BLOCKCHAIN SYSTEM

In blockchain system, someone send you the money to your public address which is basically the hash of your public key and some additional information. As we have seen above, the public key is derived mathematically from your private key.

Public and private keys are both large integer values and they are represented, for brevity's sake, via the Wallet Import Format (WIF) which consists of letters and numbers. A sample private key and public address looks like this in WIF:

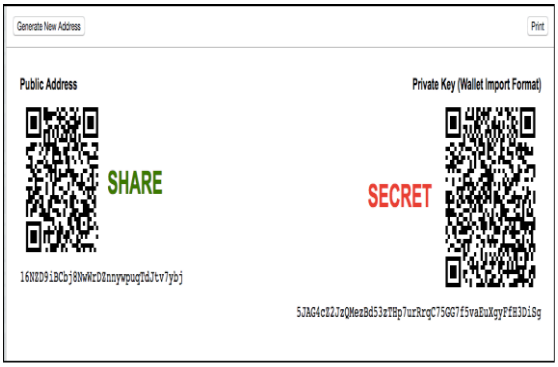

Figure 5: Public and private keys in blockchain

Obviously, you shouldn't share your private key with the world like we just did! The private key is used to sign off on the transaction that the user wants to do. So, if someone has access to your private key, they can sign off on transactions using your private key and, in essence, steal from you. Also, as you can see, the private key is longer than the public address.

The process of public key derivation from private key is explained here under

Suppose, Alice wants to generate her keys so that she can conduct transactions on the blockchain. This is what she will do:

- First, she will generate her 256-bit private key. She can either do so manually OR she will use an auto-generator. This is an example of a private address generator that you can find in a wallet-generator.net:

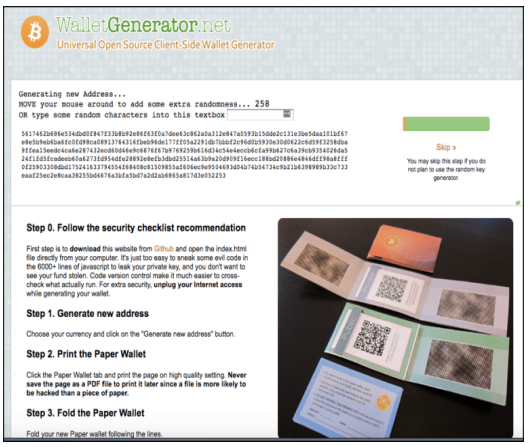

Figure 6: Process of public key derivation

- Next, she will have to generate the public address which the algorithm inside that wallet will do automatically by following these steps.
- First, her private key will be parsed through the SHA 256 hashing algorithm to get a hash.
- Then hash will be parsed through the RIPE MD 160 function and a new hash will be generated and a copy of it will be kept aside, let's call this PART A.
- Then the hash will be hashed through SHA 256 to generate another hash.
- Then the new hash will be hashed through SHA 256 again to generate another hash. The first 7 bits of this hash will be saved, let's call it PART B.
- PART A and PART B will be added up and the result is the public address.

It is infeasible for this process to be reversed in a way that the public address can be used to generate the private key. It will take the world's most powerful computer 4000000000000000000000000000000000 years to complete this calculation! Safe to say your address and key are secure.

CONCLUSION

Public key cryptography asymmetric cryptography is one of the backbones of cryptocurrency. It is impossible to even imagine how bitcoin and ethereum would have been secure without it. Cryptographic protection of the blockchain has withstood all attempts at data-

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 21
October 2018

tampering, and there have been many. Moreover, new cryptocurrencies are implementing even more secure methods of cryptography, some of which are already quantum-proof and thus protected from potential future threats.

REFERENCES

[1] Schneier, Bruce. Applied cryptography. Ed 2nd., JohnWiley & Sons, New York, 1996.

[2] https://blockgeeks.com/guides/cryptocurrencies-cryptography/

[3] https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/

[4] https://medium.com/vandal-press/to-understand-blockchains-you-should-understand-cryptographic-hashes-first-for-normies-93bc7645e816

[5] https://www.investinblockchain.com/what-is-cryptography/ K. Elissa, "Title of paper if known," unpublished.